UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of a cellular device bearing phone number 310-871-9936 with IMSI number 310280098651307 registered to West Pride Trucking LLC	)))	Case No. 2:24-MJ-3728

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-2

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 549	Removing Goods from Customs Custody
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 545	Smuggling
18 U.S.C. § 542	Entry of Goods By Means of False Statement

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

Martina Doino, HSI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

The Hon. Alka Sagar, Magistrate Judge
Printed name and title

AUSA: Colin Scott (x3159)

ATTACHMENT A-2

ITEM TO BE SEARCHED

A cellular device bearing phone number 310-871-9936 with IMSI number 310280098651307 (the "**SUBJECT DEVICE**") registered to West Pride Trucking LLC.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband fruits, or instrumentalities of violations of 18 U.S.C. § 549 (Removing Goods from Customs Custody); 18 U.S.C. 371 (Conspiracy); 18 U.S.C. § 545 (Smuggling Goods into the United States); and 18 U.S.C. § 542 (Entry of Goods by Means of False Statements) (collectively, the "SUBJECT OFFENSES"), namely:

a. Any counterfeit or duplicate high security bolt seals

b. Any counterfeit items or prohibited food items deemed not inspected by CBP;

c. All records related to M&J International Services LLC;

d. All communications between Marco Antonio Tarango and Andrew Joseph Rodriguez-Albinez regarding the diversion of cargo containers;

e. Data, records, documents, programs, applications or materials relating to the smuggling of goods , including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times of smuggled goods were bought, sold or otherwise distributed and any materials, documents, or records that are related to the sale, purchase, receipt, or possession of any smuggled goods, including books, receipts, photographs, bills of sale, shipping receipts, identification cards, bank

statements, and correspondence discussing, requesting or confirming purchase, sale or shipment;

f. Tools, paraphernalia, or materials used as a means of packaging, selling, or distributing smuggled goods.

g. Any indicia of occupancy, residency, or ownership of the SUBJECT PREMISES and things described in the warrant, including forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

h. Items of personal property reflecting names, addresses, telephone numbers, or communications of members or associates involved in the smuggling activities, including personal telephone books, address books, telephone bills, photographs, videotapes, facsimiles, personal notes, cables, telegrams, receipts, and documents and other items;

i. Any bills and/or subscriber documents related to digital devices used to facilitate the SUBJECT OFFENSES;

j. United States currency, money orders, or similar monetary instruments over $1,000 or bearer instruments worth over $1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds);

k. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, rubber bands, plastic or shrink wrap, and plastic sealing machines;

l. Records, documents, programs, applications, or materials reflecting or relating to payment, receipt, concealment, transfer, or movement of money, including but not limited to bank account records and other financial institution records, wire transfer records, receipts, safe deposit box keys and records, and notes;

m. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to U.S Customs and Border Protection concerning the importation of merchandise.

n. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to logistics companies or transporters of cargo containers.

o. Records, communications, information, documents, programs, applications, or materials relating to communications made or records submitted to any/all customs house broker(s).

p. For all digital devices, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

q. For all digital devices, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any digital devices used to facilitate the SUBJECT OFFENSES and all telephone numbers

accessed through any push-to-talk functions, as well as all received or missed incoming calls;

r. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email or social media communications or other text or written communications sent to or received from any digital device;

s. Contents of any calendar or date book, including any calendars or date books stored on any digital devices;

t. Audio recordings, photographs, video recordings or still captured images on any digital device, phone memory cards, or other storage related to the purchase, sale, transportation, or distribution of controlled substances and listed chemicals or the collection, transfer or laundering of the proceeds of illegal activities;

u. GPS coordinates and other location information or records identifying travel routes, destinations, origination points, and other locations;

v. Any digital device used to facilitate the above listed violations and forensic copies thereof.

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

3. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

6. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed

120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress Rodriguez-Albinez's thumb- and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Rodriguez-Albinez's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

8. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the

government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

9. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Martina Doino, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security ("DHS"). Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI'), and have been so employed since December 2019.

2. I attended the HSI Criminal Investigator Training Program at the Federal Law Enforcement Training Center("FLETC"), in Glynco, Georgia. At FLETC, I received training in conducting criminal investigations into customs violations such as narcotics smuggling, interdiction, and distribution of controlled substances.

3. I am currently assigned to the Los Angeles Border Enforcement Security Taskforce ("LA BEST") in Los Angeles, California, and have been so assigned since August 2021. LA BEST is a multiagency task force aimed at identifying, targeting, and eliminating vulnerabilities to the security of the United States related to the Los Angeles/Long Beach seaport complex, as well as the surrounding transportation and maritime corridors. My responsibilities include the investigation of violations of federal criminal laws, including crimes involving money laundering, narcotics trafficking, smuggling, fraud, and immigration violations.

4. Prior to my tenure as a special agent, I was a police officer in Key Biscayne, Florida from February 2015 to May 2019.

From July 2018 to May 2019, I was a Task Force Officer ("TFO") on a High Intensity Drug Trafficking Area Task Force, where I participated in investigations into money laundering and drug trafficking crimes in South Florida. Throughout my law enforcement career, I have participated in numerous criminal investigations involving narcotics importation, exportation or distribution. Through these investigations, I am familiar with the methods and practices of drug users, drug traffickers, and drug manufacturers. I have also spoken at length with other HSI SAs and local law enforcement officers regarding methods of drug trafficking.

5. Through my investigations, my training and experience, and discussions with other law enforcement personnel, I have become familiar with the tactics and methods employed by controlled substance traffickers to smuggle and safeguard controlled substances, distribute controlled substances, and collect and launder the proceeds from the sale of controlled substances. These methods include, but are not limited to, the use of wireless communications technology, such as cellular telephones and prepaid cellular accounts; counter surveillance; false or fictitious identities; and coded or vague communications in an attempt to avoid detection by law enforcement.

II. PURPOSE OF AFFIDAVIT

6. This affidavit is made in support of applications for search warrants for the following:

a. A 2015 Navistar Truck model LF687 bearing California (CA) license plate "9G20094" with vehicle identification number 3HSDJAPR9FN618725 registered to West Pride Trucking LLC at 16503 South Dalton Avenue, Gardena, California 90247 (the "**SUBJECT VEHICLE**") as described more fully in Attachment A-1, and believed to be used by Andrew Joseph Rodriguez-Albinez ("Rodriguez-Albinez"); and

b. A cellular device bearing phone number 310-871-9936 with IMSI number 310280098651307 (the "**SUBJECT DEVICE**") believed to be used by Rodriguez-Albinez and his business West Pride Trucking LLC as described more fully in Attachment A-2.

7. The requested search warrants seek authorization to seize fruits, instrumentalities, and evidence of violations of 18 U.S.C. § 549 (Removing Goods from Customs Custody); 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 545 (Smuggling Goods into the United States); and 18 U.S.C. § 542 (Entry of Goods by Means of False Statements)(collectively, the "SUBJECT OFFENSES"), as described more fully in Attachment B. Attachments A-1, A-2, and B are incorporated by reference herein.

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all

conversations and statements described in this affidavit are related in substance and in part only.

III. Background on Cargo Container Shipments at the Port of Los Angeles

9. United States Customs and Border Protection ("CBP") is responsible for, among other things, the examination of merchandise entering the United States to ensure that it is admissible under and in compliance with United States laws, and the assessment and collection of taxes, fees, and duties on imported merchandise. In order to properly assess fees, CBP relies on a self-reporting regime in which different custom brokers inform CBP about the contents of the cargo they are trying to import into the United States.

10. Importers must supply CBP with 10 data elements when bringing goods into the United States which includes: Seller, Buyer, Importer of Record number, Consignee number, Manufacturer/Supplier, Ship To party, Country of Origin, HTSUS number, Container stuffing location, and Consolidator/Stuffer name/address).

11. CBP has local and national targeting units that targets shipments that may yield prohibited items.

12. Once cargo has been selected for CBP examination, CBP will examine the contents of the cargo for discrepancies such as verifying whether the manifest is accurate, whether the goods have consistent country of origin markings, whether there are contraband or smuggled goods, as well as inspecting for environmental, and agricultural violations.

13. Once the shipment has been selected for further inspection, the container is brought to a Centralized Examination Site CES (CES) for further inspection. Containers are supposed to proceed directly to the CES after being selected for inspection.

14. The Port of Long Beach/Los Angeles handles about 40 percent of secondary inspections for the entire country. Due to the uniquely high volume at the Port of Long Beach/Los Angeles, the transportation of the containers selected for further inspection is not always controlled by CBP. In fact, the transportation of some containers selected for inspection is controlled by the broker who filed the entry/importation paperwork. In Los Angeles, custom brokers are allowed to select their own trucking company to pick up the container and take it to a CES for further inspection. This type of drayage, which is the process by which a container is unloaded, is called broker controlled drayage. The broker controlled drayage process is unique to the Los Angeles and Long Beach port. No other domestic ports have this policy in place.

15. Once cargo containers are ready for transportation at their place of origin, a high security bolt seal is affixed on the doors of the container, by the carrier, to maintain its integrity and to prevent any unauthorized person from gaining access to the cargo. The purpose of the high security bolt seal is to ensure that the cargo inside the container is not compromised. Each high security bolt seal has its own unique identification number that is documented on several import

documents. The high security bolt seal number is assigned by the vessel carrier that will transport the sea container to its destination. Below is a picture of a high security bolt seal.

16. On February 1, 2023, Customs and Border Protection ("CBP") discovered that cargo was missing from a container that had just arrived from China, and that the missing cargo was replaced, or swapped, with cargo that had clearly already entered the United States, some of which had already undergone CBP inspection.

17. This cargo swap was accomplished by using a fraudulent high security bolt seal which cloned the correctly manifested seal and its unique identification number and gave the appearance that the container had not been opened when it fact its contents had been removed and the fraudulent high security bolt seal installed.

18. Homeland Security Investigations ("HSI") opened an investigation to determine how the cargo swap occurred, what cargo was removed, and who was involved in orchestrating the breaking of the seal and removal of cargo in customs custody.

19. Since then, CBP has uncovered 102 more incidents of "cargo swapping." That is incidents, where cargo containers had their high security bolts cut and the cargo inside removed before being inspected by CBP.

20. HSI investigators have uncovered the cargo swapping scheme is a direct result of the vulnerabilities within the customer broker drayage process at the Port of Long Beach, California.

21. As described above, CBP allows customs brokers to arrange their own transportation between the port terminals and the centralized examination stations (CES) where CBP conducts inspection on imported goods that have been selected for inspection.

22. HSI has found brokers, importers, and logistic companies are not honoring CBP's explicit instructions to deliver containers directly to the CES locations.

23. The investigation has uncovered that the containers are diverted during the drayage process to prevent customs inspections and bypass custom fees.

24. Instead of being brought to the CES, HSI has found that containers are brought to an offsite location, the seal is cut, the cargo is swapped out for recycled used items. A clone seal matching the numbers of the original seal is then placed on the container. The container is ultimately delivered to be inspected by CBP.

25. HSI has concluded the smuggling scheme is a widespread industry practice which undermines the Government's authority to

inspect goods coming into the United States. As a direct result of this smuggling scheme the United States government is unable to properly secure its borders from prohibited items and impose the appropriate custom duty fees.

26. Although the exact number of swapped cargo incidents are unknown due to the sheer volume of this practice, a conservative estimate of losses would be around $50,000 dollars per diverted container in lost custom fees and fines. Based on the over 100 documented incidents, HSI believes that the scheme has resulted in approximately $5,000,000 in lost revenue to the United States.

27. In March 2024, federal agents were able to determine the cloned seals were being imported via the international mail from China by targets of the investigation. Agents began a sophisticated operation that included intercepting the air parcels, documenting the seal number, and placing CBP holds that would trigger controlled drayage on the impacted shipping containers. This operation led to the identification of more than 40 air parcels containing approximately 88 cloned seals and 79 associated sea containers.

28. To date HSI has seized more than $ 50,000,000 worth of prohibited items that would have been diverted and entered the United States without inspection. The numbers continue to grow every day has more inspections are completed and items are discovered.

IV. SUMMARY OF PROBABLE CAUSE

29. HSI investigators have determined that approximately 12 of the cargo swapping incidents described above are tied to two subjects of interest, Andrew Joseph Rodriguez-Albinez and Marco Antonio Tarango.

30. Tarango owns and operates M&J International Services LLC. The company is registered with the department of Transportation as a carrier. Rodriguez-Albinez is truck driver who works for Tarango.

31. Between January 2024 and March 2024, M&J International Services LLC and Rodriguez-Albinez have been listed as the trucking company and truck driver responsible for transporting cargo containers in at least 10 cargo swapping incidents, in which cargo containers have arrived at CBP inspection sites with tampered seals. Rodriguez-Albinez has been listed as the truck driver for these incidents. Rodriguez-Albinez has utilized the **SUBJECT VEHICLE** on each of these occasions.

23. Phone tolls for M & J International Services LLC show frequent communication with the **SUBJECT DEVICE** during period of time when the cargo containers have been swapped.

24. Bank account records from a Chase business account belonging to M&J International Services LLC show various payments utilizing Zelle, a peer-to-peer payment method, to Rodriguez-Albinez on at least two separate dates for amounts far above the industry norms for the when container diversions occurred. Therefore, I believe there is likely to be evidence

of the SUBJECT OFFENSES in the **SUBJECT VEHICLE** and **SUBJECT DEVICE**.

V. STATEMENT OF PROBABLE CAUSE

A. The SUBJECT VEHICLE is Linked to a Cargo Swap Event on July 25,2023

25. Based on my review of customs records, I know that on July 25, 2023, a shipping container numbered GLDU9359245, (the "245 Container") arrived in the United States at the Port of Los Angeles via the cargo vessel "Ever Leading." Prior to its arrival at the Port, on July 26, 2023, CBP placed an inspection hold on the 245 Container.

26. On August 18, 2023, CBP installed a global positioning system tracker ("GPS") on the 245 Container[1] at the Arnold Peter Moller ("APM") Terminal in the Port of Los Angeles.

27. On August 24, 2023, at approximately 10:26 a.m. the container was picked up by KCS Logistics at the APM Terminal. CBP officers saw an individual, later identified as Rodriguez-Albinez, pick up the 245 Container, using the **SUBJECT VEHICLE**.

28. Law enforcement then observed Rodriguez-Albinez drive past the CES in Carson, California where an inspection was scheduled to occur and take the 245 Container to an address of 15736 Valley Boulevard, City of Industry, CA 91744.[2]

---

[1] Since the 245 Container was selected for inspection and was in customs' custody until released from CBP inspection, I understand that a warrant for the placement of a GPS tracker was not needed.

[2] On June 20, 2024, the Honorable Magistrate Judge Rozella A. Oliver, signed a warrant to search this location in case number 24-MJ-3684.

29. Based on discussion with other federal agents, I understand that federal agents then observed the **SUBJECT VEHICLE** back up against a warehouse in a manner that suggested it was being unloaded. Approximately 5 hours later law enforcement saw the 245 Container go back to the CBP Price Transfer CES.

30. Upon arrival at the Price Transfer CES, Task Force Officer ("TFO") Yit interviewed Rodriguez-Albinez about the 245 Container.

31. Documents provided by Price CES warehouse, which I reviewed, show Rodriguez-Albinez listed as the driver for the 245 Container. The **SUBJECT VEHICLE** was listed on the container information sheet maintained by Price CES as the truck that was used to drop off the 245 Container.

B. Interview of RODRIGUEZ-ALBINEZ on July 25, 2023

32. From conversations with law enforcement, I know that TFO Yit inspected the bolt seal on the 245 Container and noted that there were sections where the unique identifying number was shaved/scraped off, and the number manifested to this container was laser etched over to appear like the authentic, properly affixed seal manifested to the container in import documentation and systems. TFO Yit determined the seal had been tampered with.

33. During the interview, Rodriguez-Albinez stated that he owned his own truck, the **SUBJECT VEHICLE**, but works for a dispatcher named "Marco."

34. Rodriguez-Albinez told law enforcement that he was a truck driver and has been driving for the last 2 years.

35. Rodriguez-Albinez stated he gets paid approximately $150-$250 per job, depending on the destination.

36. Rodriguez-Albinez stated he picked up the 245 Container in the **SUBJECT VEHICLE** from the APM seaport terminal and was instructed by Tarango to take it to a yard in Compton prior to bringing it to the Price Transfer CES.

37. Rodriguez-Albinez gave TFO Yit consent to search the **SUBJECT DEVICE**. Rodriguez-Albinez showed TFO Yit a text message conversation with phone number 626-475-6277, which I reviewed, saved under "Marco JWD."

38. I know from a database search that I conducted on June 20, 2024, that this is the phone number listed for M&J International Services LLC's on its Department of Transportation profile page.

39. The text messages stated, "Tomorrow morning dispatch, Grab own chassis 40FT, Head to APM, Load out, GLDU9359245, Appt 0700-0800, Appt # 576443, Under KSAE, KCS logistics," and "Once you drop at Fontana Grab load from Industry valley GLDU Return to Price Transfer Tracker 25925 Under KCS logistics."

40. Based on my knowledge of the investigation, these text messages show Tarango directed Albinez-Rodriguez to pick-up the 245 Container from the seaport, then directed it be picked up from somewhere identified as "Industry Valley," which can reasonably be discerned to be 15736 Valley Boulevard, City of

Industry, CA 91744, where, as described above, the container was observed being unloaded.

C. The Subject Vehicle Is Used To Divert Another Cargo Container On February 6, 2024

41. I know from reviewing law enforcement records, that on January 25, 2024, container number SEKU9337193 (the "193 Container") arrived at the Port of Long Beach, California aboard the Hyundai Saturn vessel from Shanghai, China. On January 18, 2024, CBP placed an examination hold to inspect the contents of that container.

42. On February 6, 2024, the 193 Container arrived at the Price Transfer CES located in Carson, California at approximately 3:00 a.m.

43. According to the terminal out gate ticket[3], I know that the 193 Container was picked up at the APM Terminal by the **SUBJECT VEHICLE** inside the Port of Long Beach on February 5, 2024, at approximately 8:55 p.m.

44. Based on my review of the in-gate ticket[4] from the Price CES, I know that the container took almost six hours and seven minutes to reach the Price CES. The total distance between the Price Centralized examination station and the APM Terminal is approximately 11 miles, with an estimated 25-minute drive time at peak traffic. Because it took the 193 Container

[3] A terminal in gate ticket is a document provided to truck drivers when entering a terminal that includes the container number in their possession and time stamps of their arrival.

[4]

over six hours to make it to the Price CES, I believe that it was diverted and unloaded at a different location prior to being delivered to the Price CES.

45. I know from reviewing law enforcement reports that on February 7, 2024, CBP Officers inspected the contents of the 193 Container and determined about 50 percent of the cargo was personal protective equipment and medical gowns. Additionally, CBP Officers discovered marked boxes that they recognized from a previous cargo swapping incident that occurred on August 31, 2023.

46. I reviewed records provided by Price CES showing the truck driver for the 193 Container as Rodriguez-Albinez, and M&J International Services LLC was listed as the trucking company. According to the records, Rodriguez-Albinez was driving the **SUBJECT VEHICLE** when he dropped off the 193 Container for inspection.

47. I know from my investigation that the **SUBJECT VEHICLE** has likely carried cargo containers for at least nine other cargo swapping events. I came to this conclusion by comparing in-gate and out-gate times for cargo containers that were transported by the **SUBJECT VEHICLE** which all took far longer than I would anticipate based upon my knowledge of traffic near the Port of Long Beach and Los Angeles.

D. The SUBJECT DEVICE and SUBJECT VEHICLE are Operated by RODRIGUEZ-ALBINEZ

48. I reviewed AT&T subscriber records for the phone number associated with the **SUBJECT DEVICE.** The records show the number 310-871-9936 was registered to Andrew Albinez at 16503 South Dalton Avenue, Gardena, CA 90247.

49. The email listed on the billing account was westpride.trucking701@gmail.com.

50. California Department of Motor Vehicles registration checks show the **SUBJECT VEHICLE** is registered to West Pride Trucking LLC at 16503 South Dalton Avenue, Gardena, CA 90247.

51. West Pride Trucking LLC is a trucking company registered to Rodriguez-Albinez with the Department of Transportation. The company is registered by the Department of Transportation as a carrier with an address of 16503 South Dalton Avenue, Gardena, CA 90247. The phone number listed on the company profile is the same as the **SUBJECT DEVICE.**

52. I reviewed toll records for the **SUBJECT DEVICE** obtained from AT&T. The Tolls show the number 6277, which I know was saved under the contact "Marco JWD" as describe above, was in contact with the **SUBJECT DEVICE** during several cargo swapping events identified by HSI, including events on February 22nd, 23rd, 27th, 28th of 2024.

E. M&J International Services LLC Paid Albinez-Rodriguez Above Market Price For Delivery Services

53. I reviewed documents obtained from JP Morgan Chase Bank, N.A for Chase business account number 886758181 belonging

to M&J International Services LLC. The statements returned reflected the banking activity which occurred between August 2022 through October 2023.

54. Documents show the account was opened by Tarango on or around August 2022.

55. Banking statements show three Zelle payments to "Andrew" dated August 14, 2023, for $3,200; August 30, 2023, for $2,970.00; and $100.00 on the same day. The dates coincide with two identified cargo diversion incidents where Albinez-Rodriguez picked up containers under KCS Logistics and delivered them to the Price CES facility.

56. Based on a public bulletin published by the CBP on January 18, 2024, about the Price CES facility trade and enforcement examination fee schedule, I know the flat rate to transport one 20' to 53' Containers one way is approximately $155. This figure is the typical price for the drayage of containers to the CES from the port based on current industry prices. Therefore, the payment Tarango sent to Rodriguez-Albinez is significantly relatively higher than normal industry prices. Therefore, I believe that Tarango is compensating Rodriguez-Albinez with an increased payment for engaging in illegal activity.

IV. TRAINING AND EXPERIENCE ON CUSTOM OFFENSES

57. Based on my training and experience and familiarity with investigations custom violations conducted by other law enforcement agents, I know the following:

a. Importing smuggled goods is a business that is typically lucrative and involves numerous co-conspirators, from the customs brokers to the delivery drivers, to warehouse workers.

b. Custom violators often maintain books, receipts, notes, ledgers, bank records, and other records relating to the importation, transportation, ordering, sale and distribution of smuggled goods at their businesses and residences and in their cars. The aforementioned records are also often maintained where the smugglers have ready access to them, such as on their cell phones and other digital devices. These cell phones and other digital devices are often kept at businesses, residences, and cars and on the person of those engaged in this activity.

c. Communications between importers and costumers buying and selling smuggled goods take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the smuggled goods between the seller and the buyer, the negotiation of price. In addition, it is common for people engaged in customs violations to have photos and videos on their cell phones of the contents of a container and the goods. These cell phones are often kept at businesses, residences, and cars and on the person of those engaged in this activity.

d. Custom violators often keep the names, addresses, and telephone numbers of their associates at their residences and businesses and on their digital devices. Violators often keep

records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

58. As used herein, the term "digital device" includes the **SUBJECT DEVICE.**

59. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

60. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data in a short period of time for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

61. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Rodriguez-Albinez's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of Rodriguez-Albinez's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

62. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any

identifying information on the exterior of the device. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located during the execution of the search: (1) depress the person's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

63. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

64. For all the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of Subject offenses will be found in the **SUBJECT DEVICE** and **SUBJECT VEHICLE**, as described in Attachment A-1 and A-2.

Subscribed to and sworn before me
this 21 day of June, 2024.

_____

HONORABLE ALKA SAGAR
UNITED STATES MAGISTRATE JUDGE